19 Marzo 2026

Confini di vetro: geopolitica dei dati e il mito del mondo senza frontiere

Di Adriana Augenti

Abstract

Nell'era globale i confini sono diventati trasparenti. Non sono caduti — si sono fatti di vetro. Cavi sottomarini con proprietari e giurisdizioni, decisioni di adeguatezza che certificano equivalenze traballanti, brevetti che ridisegnano il potere più di qualsiasi trattato: li attraversiamo ogni giorno senza vederli, finché non proviamo a far valere un diritto. L'Europa ha costruito le regole più sofisticate del mondo, ma regola ciò che non possiede. La via d'uscita non è l'autarchia, ma la costruzione paziente di un'alternativa materiale. Le regole senza infrastrutture sono vetri senza telaio: bellissime, fragilissime, destinate a cadere.

Indice

Introduzione – Il mito del mondo senza frontiere

Alla fine del secolo scorso, la digitalizzazione era salutata come la forza che avrebbe appiattito il mondo. Una rete globale, de-territorializzata, in cui i confini fisici sarebbero diventati reliquie del passato e la cittadinanza si sarebbe fatta cosmopolita, immateriale, libera. Era una promessa bellissima. Non era falsa — era incompleta.

I confini non sono caduti. Si sono fatti trasparenti.

> Chiamiamoli confini di vetro. Li attraversiamo ogni giorno senza vederli: quando accettiamo un'informativa privacy senza leggerla, quando i nostri dati sanitari finiscono su un server che risponde a leggi che non conosciamo, quando un brevetto depositato dall'altra parte del mondo decide quali tecnologie potremo usare. Il vetro ha questa proprietà: ci vedi attraverso, ti illude che non ci sia nulla, ma provaci a passare. Ti ferma.

Perché questa è la realtà che il mito del mondo senza frontiere nascondeva: nel digitale non esistono confini geografici tradizionali, ma esistono proprietari. E i proprietari hanno giurisdizione.

L’articolo 45 del GDPR affida alla Commissione Europea il potere di certificare questa trasparenza. Le decisioni di adeguatezza — quegli atti con cui Bruxelles dichiara che un paese terzo offre un livello di protezione dei dati “sostanzialmente equivalente” a quello europeo — sono il sigillo ufficiale sui confini di vetro. Sostanzialmente equivalente: formula che non significa uguale. Significa abbastanza simile perché possiamo far finta che vada bene. E la distanza tra “equivalente” e “abbastanza simile” è esattamente lo spazio in cui si giocano i rapporti di forza tra chi possiede le infrastrutture e chi possiede solo le regole.

Proviamo ad attraversare quei confini. Partiamo dall’infrastruttura materiale — i cavi, i server, la geografia fisica del potere digitale. Saliamo alle finzioni diplomatiche — le decisioni di adeguatezza, il sistema che certifica equivalenze che non esistono. Arriviamo alla *weaponization* della proprietà intellettuale — i brevetti, le guerre tecnologiche, l’uso dei diritti immateriali come strumento di proiezione geopolitica. E chiudiamo con una domanda che il diritto europeo non può più eludere: cosa significa avere le regole più ambiziose del mondo se non possiedi le infrastrutture su cui quelle regole dovrebbero operare?

> I confini di vetro hanno una proprietà: sono trasparenti, ma non sono invisibili. Si possono vedere, misurare, contestare. A condizione di sapere che sono lì.

L’architettura materiale del potere

Prima di parlare di diritto, parliamo di fisica.

Il cloud non esiste. Esiste un’infrastruttura di cavi, server e data center che qualcuno possiede, qualcuno alimenta e qualcuno controlla. La parola “cloud” — nuvola — è un capolavoro di marketing linguistico: evoca leggerezza, ubiquità, immaterialità, nascondendo il fatto che oltre il 95% del traffico dati intercontinentale passa in realtà attraverso cavi sottomarini in fibra ottica. Non satelliti, ma strutture fisiche posate sul fondo degli oceani, vulnerabili alle ancore, ai terremoti e, sempre più spesso, alle decisioni politiche e militari.

La mappa di questi cavi è la mappa del potere digitale.

Fino ai primi anni Duemila, appartenevano a consorzi di telecomunicazioni statali o regolamentati. Oggi la geografia degli abissi ha cambiato padrone: oltre il 70% della capacità sottomarina internazionale è controllato dai cosiddetti *hyperscaler* americani (Google, Meta, Amazon, Microsoft). Google, da sola, possiede o co-possiede trentaquattro cavi sottomarini, Meta ne ha sedici, mentre il totale dei cavi delle big tech è passato da venti nel 2017 ai quasi sessanta attuali. Il fornitore del servizio è anche il proprietario del tubo.

E chi possiede il tubo ha in mano un’arma formidabile. La Cina lo ha capito lanciando la sua *Digital Silk Road*, un progetto infrastrutturale globale per costruire la propria rete di cavi e sfuggire al controllo occidentale. Gli Stati Uniti rispondono bloccando preventivamente i collegamenti sottomarini verso Hong Kong per motivi di sicurezza nazionale.

Ma questa competizione non è solo economica: è diventata militare. Siamo entrati nell’era delle *Cable Wars*. I cavi sottomarini sono diventati bersagli strategici per operazioni di sabotaggio o guerra ibrida, come dimostrano i misteriosi tranciamenti di cavi nel Mar Baltico, dove l’infrastruttura europea è costantemente monitorata e minacciata da flotte ombra russe o navi cargo sospette. Se si taglia un cavo, si fermano le transazioni finanziarie per migliaia di miliardi; si paralizza un Paese senza sparare un colpo.

> In questo scontro titanico, l'Europa occupa una posizione di vulnerabilità cronica. Il diritto europeo ha costruito il sistema di protezione dei dati più sofisticato del mondo, ma l'UE importa oltre l'80% dei prodotti e servizi digitali che utilizza, e non possiede quasi nulla dell'infrastruttura fisica su cui quei dati viaggiano.

Liu Cixin, nella sua trilogia del *Problema dei Tre Corpi*, descrive un sistema fisico in cui tre forze gravitazionali si influenzano in modo caotico e imprevedibile, senza una soluzione stabile[1]. I tre corpi di oggi si chiamano Stati Uniti, Cina e le piattaforme globali degli *hyperscaler*. L'Europa, in questa metafora, non è un quarto corpo: è un satellite che orbita intorno al sistema cercando di stabilizzarlo con la sola forza delle proprie regole.

> Il primo confine di vetro è questo: la distanza tra la sovranità che proclamiamo e l'infrastruttura che non controlliamo.

Finzioni diplomatiche e il teatro della sovranità

Se l'infrastruttura fisica ci sfugge, la dipendenza che ne deriva non è solo materiale, ma profondamente giuridica.

Il CLOUD Act statunitense stabilisce che le autorità americane possono richiedere a qualsiasi azienda soggetta alla giurisdizione USA di fornire i dati in suo possesso, ovunque quei dati siano fisicamente conservati. Se i server sono a Francoforte, a Dublino o a Milano, poco importa: se l'azienda è americana, i dati rispondono alla legge americana[2]. A questo si aggiunge il FISA Section 702, che autorizza la sorveglianza senza mandato delle comunicazioni di cittadini non americani. L'extraterritorialità, in questo impianto, non è un'eccezione: è il design del sistema.

Il *sovereignty-washing* è la risposta cosmetica del mercato a questa contraddizione. Di fronte alle preoccupazioni europee, i colossi statunitensi lanciano iniziative come il "*Microsoft EU Data Boundary*" o stringono partnership con operatori locali — come Bleu in Francia (joint venture tra Orange, Capgemini e Microsoft) o Delos in Germania (sussidiaria SAP su infrastruttura Microsoft). Il messaggio rassicurante è che i dati risiederanno fisicamente in Europa. Eppure, se le chiavi di crittografia e gli aggiornamenti software restano sotto il controllo delle case madri negli Stati Uniti, il cordone ombelicale con il CLOUD Act non si spezza.

> Questa non è sovranità. È teatro. I dati dormono in Europa, ma si svegliano americani.

E siccome non possiamo possedere l'infrastruttura, né spezzare questo legame giurisdizionale, abbiamo provato a certificare chi ci passa sopra. È il sistema delle decisioni di adeguatezza: la via maestra con cui la Commissione Europea certifica che un Paese terzo offre un livello di protezione "sostanzialmente equivalente" al nostro.

Partiamo dai numeri: l'UE ha adottato decisioni di adeguatezza per soli diciassette Paesi e territori su quasi duecento Stati nel mondo. Il resto del pianeta non è "adeguato". I dati ci vanno comunque, attraverso clausole contrattuali standard, norme vincolanti d'impresa o le deroghe dell'art. 49 — strumenti che, dopo Schrems II, richiedono tutti un Transfer Impact Assessment (TIA). In pratica, chiunque abbia compilato un TIA sa che si tratta di una liturgia: si parte dalla necessità di trasferire il dato — perché il fornitore è quello e l'alternativa europea non esiste — e si lavora a ritroso per giustificare il trasferimento. Le misure supplementari diventano un esercizio di stile per certificare non la sicurezza del trasferimento, ma la buona fede del Titolare nel fingersi sicuro. Un sistema che chiede all'ospedale o all'azienda di Bari di fare ciò che la Commissione stessa fatica a fare: valutare la compatibilità di un intero ordinamento straniero con i diritti fondamentali europei.

Ma anche guardando alle stesse diciassette decisioni di adeguatezza, la parola “equivalente” diventa spesso un esercizio di generosità interpretativa, piegata alla *realpolitik*. Israele è adeguato dal 2011, e non è mai stato formalmente declassato nonostante l’esportazione globale dello spyware Pegasus, l’uso massiccio di sorveglianza biometrica nei territori occupati, e un contesto bellico in cui organizzazioni internazionali hanno documentato gravi violazioni dei diritti umani — quegli stessi diritti che l’art. 45(2) GDPR elenca tra i criteri per la valutazione di adeguatezza. Il Regno Unito è rimasto adeguato post-Brexit, con recente rinnovo fino al 2030, nonostante il suo *Investigatory Powers Act* sia stato giudicato problematico dalla Corte EDU. Il Giappone è adeguato grazie a un accordo politico di reciprocità, pur avendo una cultura della *data protection* e del consenso strutturalmente diversa dalla nostra.

> Ma il vero conflitto, la vera faglia sismica, è quella con gli Stati Uniti. La saga è nota: il Safe Harbor è stato invalidato nel 2015 (*Schrems I*), il Privacy Shield è crollato nel 2020 (*Schrems II*). In entrambi i casi, la CGUE ha statuito che la sorveglianza di massa statunitense è un’architettura costituzionale strutturalmente incompatibile con i diritti europei.

Nel quadro attuale navighiamo nel terzo tentativo: il *Data Privacy Framework* del 2023, basato su un Executive Order di Joe Biden che ha istituito un *Data Protection Review Court* per offrire un meccanismo di ricorso. Recentemente, nel settembre 2025, il Tribunale dell’Unione Europea ha respinto il primo ricorso contro il DPF presentato dal politico francese Philippe Latombe, stabilendo in primo grado che il DPRC possiede garanzie sufficienti di indipendenza. Le 3.400 aziende americane certificate adesso tirano un sospiro di sollievo, ma l’incertezza è cronica. Tutti sanno che la vera scure attesa è quella della CGUE, storicamente molto più severa del Tribunale di primo grado, verso cui Max Schrems e la sua associazione *Noyb* stanno già affilando le armi per un inevitabile “Schrems III”.

Le decisioni di adeguatezza si svelano così per quello che sono: atti politici presentati come valutazioni tecniche. Sono l’architettura che normalizza il potere, proprio come aveva intuito Stefano Rodotà con decenni di anticipo. Il “corpo elettronico” teorizzato da Rodotà — l’insieme dei dati che ci rappresentano — è ormai ostaggio di un controllo distribuito che non ha bisogno di essere autoritario per essere pervasivo, ma si legittima attraverso compromessi diplomatici.

> Questo secondo confine di vetro funziona così. È trasparente e non ferma l’economia: i dati attraversano l’oceano in tempo reale. Ma la nostra capacità di *enforcement*, la nostra possibilità effettiva di far valere un diritto, si schianta contro quel vetro non appena il dato tocca un server in Virginia.

L’arma invisibile e la frammentazione della rete

Nel 1984, un programmatore sovietico di nome Alexei Pajitnov creò un gioco nel suo tempo libero, su un computer dell’Accademia delle Scienze di Mosca. Pezzi geometrici che cadono, tu li incastri. Lo chiamò *Tetris*. Non poteva immaginare che quel gioco sarebbe diventato il campo di battaglia di una guerra combattuta senza un solo proiettile — una guerra di licenze, diritti e contratti che avrebbe coinvolto multinazionali e governi. Pajitnov non possedeva nulla di quello che aveva creato, perché in Unione Sovietica la proprietà intellettuale individuale semplicemente non esisteva. La posta in gioco non era il videogioco in sé, era il principio: chi ha il diritto di possedere un’idea nata nella testa di un uomo che non ha il diritto di possederla?

Tetris è il prototipo perfetto di ciò che chiamiamo *weaponization* della proprietà intellettuale: l’uso dei diritti immateriali come strumento di proiezione geopolitica. Con una differenza cruciale: negli anni Ottanta ci si scontrava per un videogioco, oggi la guerra si combatte per i semiconduttori.

Nell’ottobre 2022, gli Stati Uniti hanno introdotto restrizioni chirurgiche alle esportazioni verso la Cina dei chip più avanzati e delle macchine per produrli. L’obiettivo dichiarato era la sicurezza nazionale; l’effetto reale è stato ridisegnare la mappa del potere tecnologico globale con un tratto di penna.

In questo scontro, i Paesi Bassi sono diventati un attore geopolitico cruciale perché ASML, con sede a Veldhoven (poco meno di 50mila abitanti), è l’unica azienda al mondo capace di produrre le macchine per la litografia necessarie a fabbricare i chip del futuro. Washington ha chiesto e ottenuto che l’Olanda bloccasse quelle esportazioni. Il confine di vetro, in questo caso, non è passato per gli abissi oceanici, ma per una fabbrica nel Brabante, dimostrando che un embargo tecnologico è, innegabilmente, anche un’arma economica.

La Cina ha risposto come fanno le grandi potenze messe all’angolo: accelerando sull’autosufficienza e arrivando a superare gli Stati Uniti per numero di brevetti depositati nel settore dell’intelligenza artificiale.

L’Europa, in questa partita, occupa una posizione peculiare. Ha il proprio Chips Act, ma regola un mercato in cui è prevalentemente acquirente, non produttrice.

> Regolamentare ciò che dipende da altri è un puro esercizio di sovranità limitata: un concetto che il diritto internazionale conosce bene, ma che nel dibattito tecnologico facciamo ancora fatica a nominare.

Il sistema dei brevetti, nato per proteggere l’inventore, è mutato. È diventato una leva. Maurizio Ferraris, filosofo che cartografa il rapporto tra tecnologia e potere, ha dato a questo meccanismo un nome: *mobilitazione totale**[3]***. Siamo tutti arruolati, spesso inconsapevolmente, nella produzione di dati. Ogni nostro clic è lavoro che genera un dato che qualcun altro possiede e trasforma in controllo. E quando questo potere viene usato come arma di esclusione, le reazioni sono dirompenti.

Siamo ancora nel 2022 quando le sanzioni occidentali hanno tagliato alla Russia l’accesso alle tecnologie protette. Mosca ha risposto ignorando la proprietà intellettuale e legalizzando la pirateria[4]. Il diritto si è rivelato per quello che è: un’estensione della politica estera con altri mezzi. Clausewitz, se avesse vissuto nell’era digitale, avrebbe apprezzato la coerenza.

Questa conflittualità sta frammentando la struttura stessa della rete globale. La localizzazione dei dati — l’obbligo imposto da paesi come Russia, Cina, India e Indonesia di conservare i dati dei cittadini su server fisicamente situati entro i confini nazionali — è la risposta sovranista alla globalizzazione digitale. È il fenomeno dello *Splinternet*: la rete si divide in ecosistemi paralleli separati da barriere normative che riflettono fratture geopolitiche. Se non puoi controllare dove vanno i tuoi dati perché non possiedi i cavi, provi almeno a innalzare un confine di vetro per controllare dove restano.

> L’Intelligenza Artificiale è il nuovo, definitivo terreno di conflitto. L’Europa ha partorito l’AI Act compiendo uno sforzo indubbiamente storico. Tuttavia, i dataset immensi su cui questi modelli vengono addestrati attraversano i nostri confini di vetro prima ancora che le norme vengano applicate, e i brevetti sulle architetture strategiche appartengono quasi interamente ad aziende americane e cinesi.

Alexei Pajitnov dovette aspettare il 1996 e il crollo dell’Unione Sovietica per fondare una società e ottenere una parte dei diritti sul suo videogioco. Il confine di vetro, nel suo caso, era un impianto giuridico che negava l’esistenza stessa della proprietà intellettuale. Oggi ci scontriamo contro il confine opposto: un eccesso di proprietà intellettuale altrui che diventa strumento di controllo ed esclusione.

> Il terzo confine di vetro è questo: scoprire che le nostre sofisticatissime regole su brevetti, diritti e concorrenza valgono ben poco, quando i brevetti strategici e le

> macchine per farli funzionare appartengono ad altri.

L’Europa al bivio e la rottura del vetro

Ricapitoliamo cosa sappiamo.

Sappiamo che il 95% del traffico dati globale passa attraverso cavi sottomarini oceanici controllati in larghissima parte da monopoli privati.

Sappiamo che la diplomazia tenta di rammendare le crepe giurisdizionali con decisioni di adeguatezza traballanti e costantemente *sub iudice*.

Sappiamo che la proprietà intellettuale e i microchip sono diventati le trincee di una nuova guerra fredda.

I confini, insomma, non sono mai caduti: si sono semplicemente fatti di vetro.

L’Europa ha cercato di governare questo ecosistema con la sola forza del diritto. Il GDPR, l’AI Act, la Direttiva NIS2 e il DORA sono architetture normative invidiate e spesso imitate nel mondo. L’effetto Bruxelles esiste. Ma c’è una contraddizione strutturale che, come giuristi e cittadini, non possiamo più eludere: **l’Unione Europea produce le regole più ambiziose del pianeta per proteggere i dati, ma dipende per la propria infrastruttura materiale da aziende che a quelle regole obbediscono solo fino a prova contraria.** Regolamentare da Bruxelles macchine e algoritmi che fisicamente risiedono o dipendono da San José o Shenzhen è, nei fatti, esercizio di sovranità limitata.

Come si esce da questa dipendenza?

> La risposta non è l’autarchia protezionista, impraticabile e anacronistica, ma la costruzione paziente di un’alternativa materiale. L’imminente *Cloud and AI Development Act*, la direttiva europea in discussione per i prossimi anni, rappresenta un primo, tardivo giro di boa. L’obiettivo del CADA è di triplicare la capacità dei data center sul territorio dell’Unione e di blindare i carichi di lavoro critici (come quelli della pubblica amministrazione), imponendo che siano gestiti esclusivamente su infrastrutture immuni a giurisdizioni extra-europee. È il tentativo di passare dalla *moral suasion* delle certificazioni volontarie a obblighi infrastrutturali vincolanti.

Eppure, la vera sovranità digitale spesso non scende dall’alto dei grandi piani continentali, ma sale dal pragmatismo delle amministrazioni locali. L’antidoto reale al sovereignty-washing delle Big Tech non è la creazione di un altro monopolio, ma può essere rappresentato dall’adozione strutturale dell’open source. Ne è prova tangibile la scelta del Land tedesco dello Schleswig-Holstein, che nel 2025 ha completato la migrazione di circa 30.000 postazioni pubbliche da Microsoft Office e Windows verso LibreOffice e Linux. Non è un esperimento isolato: il Ministero dell’Interno tedesco ha lanciato *openDesk*, una suite open source per sostituire Microsoft 365; l’esercito austriaco ha rimosso Office da 16.000 postazioni militari; la Francia ha vietato Teams, Zoom e Google Meet per le comunicazioni ministeriali. È un atto di indipendenza radicale: riprendere possesso del codice significa spezzare quell’aggancio giurisdizionale con leggi extraterritoriali come il CLOUD Act. In quei server, finalmente, i dati non solo dormono in Europa, ma obbediscono esclusivamente a leggi europee[5].

L’era globale ci aveva promesso un mondo senza frontiere. Ci ha consegnato, invece, confini senza eserciti ma intrisi di potere: linee invalicabili fatte di algoritmi, brevetti e cavi posati sul fondale oceanico.

I confini di vetro funzionano esattamente così: ci vedi attraverso, ti illudono di essere libero, ma non appena provi a far valere un diritto fondamentale o un interesse strategico, ti fermano.

Siamo davanti a una scelta ineludibile.

Le regole senza infrastrutture sono come vetri senza telaio: bellissime, fragilissime e destinate a cadere.

Sta a noi decidere se restare a guardare la trasparenza di questa gabbia, o se trovare gli strumenti per costruire finalmente il nostro telaio.

NOTE

[1] Liu Cixin, *Il problema dei tre corpi* (??, 2008, prima edizione italiana 2017). Il "problema dei tre corpi" è un classico della meccanica celeste: a differenza del sistema a due corpi, che ammette soluzioni analitiche stabili, un sistema gravitazionale a tre corpi genera traiettorie caotiche e imprevedibili. Nella trilogia, questa instabilità fisica diventa metafora delle dinamiche di potere tra civiltà in competizione.

[2] Sul CLOUD Act e i suoi effetti sui trasferimenti transatlantici, v. CGUE, 16 luglio 2020, C-311/18, *Data Protection Commissioner c. Facebook Ireland e Schrems* (*Schrems II*), spec. punti 63-65 sulle possibilità di accesso governativo ai dati. Per una lettura più circostanziata dei meccanismi operativi della norma — spesso enfatizzati oltre la loro portata effettiva — si veda AWS Security Blog, *Five facts about how the CLOUD Act actually works*, ove si chiarisce che le richieste devono comunque rispettare standard probatori stringenti e sono soggette a contestazione giurisdizionale.

[3] Maurizio Ferraris, *Mobilitazione totale,* Editore Laterza, Bari, 2015

[4] L'iperbole è voluta: la Federazione Russa ha adottato decreti che consentono la violazione di brevetti detenuti da soggetti di "paesi ostili" senza obbligo di risarcimento, e ha abolito la responsabilità penale e amministrativa per l'uso di software piratato proveniente da paesi sanzionanti.

[5] Per una ricostruzione delle iniziative europee di migrazione verso soluzioni open source: C. Morelli, *La sovranità digitale europea, quando la tecnologia diventa affare di Stato*, Altalex, 3 febbraio 2026.